Cybercrime Prevention

MARKETING PARA REDES SOCIALES

1

Email Spoofing

Enable email authentication protocols like SPF, DKIM, and DMARC to verify email sources.

2

Phishing

Always double-check email sender addresses and avoid clicking on suspicious links; verify with the organization directly.

3

Spear Phishing

Be cautious with sharing personal information online; double-check emails for personalized details before responding.

4

Crimes Emanating from User Network Newsgroup

Be cautious about sharing sensitive information in online forums; use secure, private channels when necessary.

5

Vishing

Avoid sharing sensitive information over the phone; verify the caller's identity and call back using official contact information.

6

Smishing

Don’t click on links or respond to text messages from unknown sources; verify with the organization through official channels.

7

Spamming

Use spam filters on email accounts and avoid clicking on or responding to unsolicited emails.

8

Cyber Defamation

Think before posting online; avoid spreading false information about individuals or organizations.

Más información en:
https://sites.google.com/view/owca/notes/02-19-2024

8 MORE OF THESE

1

CYBERSTALKING

Adjust social media privacy settings and be cautious about sharing location details online.

COMPUTER SABOTAGE

Regularly update and patch software to protect against vulnerabilities.

2

3

PRONOGRAPHIC OFFENSES

Be cautious when accessing online content; use reputable websites and avoid illegal downloads.

PASSWORD SNIFFING

Use strong, unique passwords and enable two-factor authentication for added security.

4

5

CREDIT CARD FRAUD

Regularly monitor bank statements; report any unauthorized transactions immediately.

PIRACY

Avoid downloading or sharing copyrighted content without permission.

6

7

INTERNET TIME THEFT

Manage time efficiently and avoid unauthorized use of work hours for personal activities.

UNAUTHORIZED ACCESSING OF COMPUTER

Use strong passwords, encrypt sensitive data, and restrict access to authorized users.

8

i dont know what to PUT HERE

1

DoS ATTAC

Implement network security measures and use a firewall to protect against denial-of-service attacks.

VIRUS ATTAC

2

Install reputable antivirus software and keep it up to date; be cautious with email attachments.

EMAIL BOMBING

Use email filters and report suspicious email activity to your email provider.

3

SALAMI ATTAC

4

Monitor financial transactions regularly for small, unauthorized deductions.

5

LOGIC BOMB

Be cautious with downloading files from unknown sources; keep software updated.

TROJAN HORSE

6

Avoid downloading files from untrusted sources; use reputable security software.

5 PASOS PARA UN PROYECTO

01

DATA DIDDLING

Regularly check and verify data integrity to detect any unauthorized changes.

02

SOFTWARE PIRACY

Use licensed software and avoid downloading cracked versions.

03

CYBERTERRORISM

Stay informed about potential cyber threats and report suspicious online activity.

04

FORGERY

Verify the authenticity of digital signatures and digital documents.

05

WEB JACKING

Regularly monitor and update website security protocols.